江民防毒墙解决方案

北京江民新科技术有限公司

二〇一五年十一月

版权声明

免责条款

本文档仅提供阶段性信息，因市场情况变化迅速，所含内容可根据产品的实际情况随时更新、修改，恕不另行通知。所以，本文档仅供参考使用，不提供任何形式的担保，如因文档使用不当造成的直接或间接损失，本公司不承担任何责任。

信息反馈

地址 :北京市海淀区蓝靛厂金源时代购物中心 B 区 2#B 座 701 室

邮编：100097

电话：010-82511166　　传真：010-82511199

邮箱：kvnet@jiangmin.com

目 录

第 1 章 概述

随着 Internet 上的应用不断丰富，网络技术的高速发展，网络已经成为新时代不可或缺的重要因素，伴之而来的各种新型未知病毒也开始层出不穷，新的混合型威胁（病毒、蠕虫、木马、僵尸网络、口令嗅探、APT 攻击等）每天都在发生，我们面临着越来越多的安全风险。这些威胁可能危及业务安全、破坏数据完整性、中断业务连续性、导致生产率下降、损坏企业声誉，以致可能造成正常工作秩序的被迫调整。

与此同时，XXX 网络信息系统在企业的运作中展现出越来越重要的作用。XXX 的员工通过内部局域网共享和交流业务数据，各分支机构之间通过专线将各个局域网连接起来构成广域网，XXX 网络又通过专线或拨号等方式与 ISP 相联，从而连接到更为广阔的 Internet。企业的绝大部分信息和关键业务数据都存储在网络的节点（计算机）中，节点之间通过网络进行通讯，方便快捷地交流信息，使得员工可以快捷高效、不受时空限制地协同工作。XXX 网络在带来信息高效流动的同时，也给病毒的高效快速传播大开了方便之门。

根据 XXX 的运维数据和经验分析，病毒一直是 XXX 面临的最大威胁。在网络运行中最常遇到的就是蠕虫、病毒、木马等。行为和目的大多具有明显特征，比如破坏系统、篡改数据、占用系统和网络带宽、疯狂传播垃圾邮件等。预防病毒、恶意攻击，防范冲击波、振荡波等蠕虫；保护 XXX 网络的信息资源和网络资源，保障关键数据的完整性、可用性、保密性和安全性，保障关键业务系统的畅通性、稳定性和可控性，已经成为 XXX 信息化持续发展的一项重要前提。

第 2 章 网络病毒现状分析

2.1 计算机病毒发展史

从一九八三年计算机病毒首次被确认以来，并没有引起人们的重视。直到一九八七年计算机病毒才开使受到世界范围内的普遍重视。我国于一九八九年在计算机界发现病毒。至今，全世界已发现近数万种病毒，并且还在高速度的增加。

由于计算机软件的脆弱性与互联网的开放性，我们将与病毒长久共存。而且，病毒主要朝着能更好的隐蔽自己并对抗反病毒手段的方向发展。同时，病毒已被人们利用其特有的性质与其他功能相结合进行有目的的活动。

病毒的花样不断翻新，编程手段越来越高，防不胜防。特别是 Internet 的广泛应用，促进了病毒的空前活跃，网络蠕虫病毒传播更快更广，Windows 病毒更加复杂，带有黑客性质的病毒和特络依木马等有害代码大量涌现。在现今的网络时代，病毒的发展呈现出以下趋势：

- **病毒与黑客程序相结合**

随着网络的普及和网速的提高，计算机之间的远程控制越来越方便，传输文件也变得非常快捷，正因为如此，病毒与黑客程序（木马病毒）结合以后的危害更为严重，病毒的发作往往伴随着用户机密资料的丢失。病毒的传播可能会具有一定的方向性，按照制作者的要求侵蚀固定的内容。

- **蠕虫病毒更加泛滥**

其表现形式是邮件病毒会越来越多，这类病毒是由受到感染的计算机自动向用户的邮件列表内的所有人员发送带毒文件，往往在邮件当中附带一些具有欺骗性的话语，由于是熟人发送的邮件，接受者往往没有戒心。因此，这类病毒传播速度非常快，只要有一个用户受到感染，就可以形成一个非常大的传染面。

- **病毒破坏性更大**

计算机病毒不再仅仅以侵占和破坏单机的资料为目的。木马病毒的传播使得病毒在发作的时候有可能自动联络病毒的创造者（如爱虫病毒），或者采取 DoS（拒绝服务）的攻击（如最近的：红色代码病毒）。一方面可能会导致本机机密资料的泄漏，另一方面会导致一些网络服务的中止。而蠕虫病毒则会抢占有限的网络资源，造成网络堵塞（如最近的 Nimda 病毒），如有可能，还会破坏本地的资料（如针对 911 恐怖事件的 Vote 病毒）。

- **制作病毒的方法更简单**

由于网络的普及，使得编写病毒的知识越来越容易获得。同时，各种功能强大而易学的编程工具让用户可以轻松编写一个具有极强杀伤力的病毒程序。用户通过网络甚至可以获得专门编写病毒的工具软件，只需要通过简单的操作就可以生成破坏性的病毒。

- **病毒传播速度更快，传播渠道更多**

目前上网用户已不再局限于收发邮件和网站浏览，此时，文件传输成为病毒传播的另一个重要途径。随着网速的提高，在数据传输时间变短的同时，病毒的传送时间会变得更加微不足道。同时，其他的网络连接方式如 ICQ、IRC 也成为了传播病毒的途径。

➢ **病毒感染对象越来越广**

到目前为止，病毒主要感染和破坏的对象还是 Windows 操作系统，但随着病毒技术发展，Unix、Linux 等操作系统下的病毒将越来越多，并且有可能出现跨系统的病毒。

2.2　病毒威胁分析

✧ **文件服务器：**文件服务器是网络环境下文件储存和访问的主要应用服务器，由于通常会有大量的文件存储到服务器中，病毒极易通过文件复制的方式在服务器中传播、复制，大量的病毒入侵可以导致文件服务器功能下降或瘫痪。

✧ **邮件服务器：**电子邮件已成为病毒传播的最大载体，任意与外界有邮件往来的邮件服务器如果没有采取有效的病毒防护措施，极易受到攻击，并会导致病毒在企业内部网中快速传播。其实邮件服务器本身不会受到邮件病毒的破坏，只是转发染毒邮件至客户信箱中，但是当客户机染毒并产生几何数量级的信件时，邮件服务器会由于在短时间内需转发大量邮件而导致性能迅速下降，直至当机。

✧ **客户机：**局域网中的工作站会受到病毒的感染，病毒的攻击方式多种多样，有通过 Internet、局域网传播、传统介质(光盘、U 盘、移动硬盘等)传播等等，一旦客户机感染病毒，便会迅速传播，并且会给日常的工作带来极大的威胁。

✧ **网络带宽：**高速传播和具有网络攻击能力的病毒，能占用有限的网络带宽，导致网络瘫痪。如：“冲击波、震荡波”就是典型导致网络瘫痪的病毒，能导致网络交换机、路由器、服务器严重过载瘫痪。

✧ **经济损失：**病毒造成的间接损失可能更大，由于病毒普遍都会对储存在计算机上的数据进行删除或破坏，病毒造成的后果是直接导致信息资产损失，同时，病毒造成的网络带宽阻塞会严重影响正常的办公。

✧ **政治影响：**电子政务网是政府办公自动化、应用信息化得平台，使得政府机构能够提供更好的公共服务。病毒造成的各种后果，直接导致政府机构提供公共服务的质量，造成政治方面的严重损失。

2.3　病毒传途径分析

当今，病毒传播方式除了通过传统的光盘、U 盘、移动硬盘传播，绝大多数传播的途径是通过网络。病毒传播方式主要有下列几种：

- **Internet 途径传播：** 这是目前病毒进入最多的途径。XXX 网络具有统一的 Internet 出口，因此，病毒可以通过 Internet 的各种应用（HTTP、FTP、MSN、QQ 等）传播到内部网络的计算机。
- **Intranet 途径传播：** XXX 内部局域网，实现应用系统信息化、办公系统自动换，这给病毒的传播提供了良好的环境，病毒可以通过各种应用和文件复制在局域网内大量传播。
- **网络邮件/群件系统：**XXX 具有自己的邮件/群件系统实施办公和信息自动化（OA），那么一旦有某个用户感染了病毒，通过邮件方式该病毒将以几何级数在网络内迅速传播，并且很容易导致邮件系统负荷过大而瘫痪。
- **文件服务器：**文件资源共享是网络提供的基本功能。文件服务器大大提高了资源的重复利用率，并且能对信息进行长期有效的存储和保护。但是一旦服务器本身感染了病毒，就会对所有的访问者构成威胁。
- **光盘、u 盘、移动硬盘：**光盘、U 盘、移动硬盘是病毒传播的传统途径，当从这些带毒的光盘、U 盘、移动硬盘复制文件后，病毒通过复制的文件入侵到用户的计算机，由于网络共享的便利性，感染病毒的计算机随时会感染其它的机器。

第 3 章 网络防病毒体系构建

3.1　传统防病毒技术的不足及反病毒发展趋势

面对现今病毒所具有的目的性和网络性的特征，传统的反病毒技术暴露出很多不足：

（1）传统的反病毒技术只能针对本地系统进行防御，其目的是为了预防病毒入侵和查杀计算机系统中已经成功进入的病毒。但这并不能保证网络中没有病毒的入侵，比如蠕虫类病毒。

（2）传统的病毒查杀技术是基于文件进行扫描的，无法适应对效率要求极高的网络查毒。传统的反病毒技术已经远远不能满足反病毒的需要。现在反病毒技术必须要能够针对病毒的网络性和目的性进行防御。

反病毒技术的发展具有以下两大趋势：

（1）防病毒体系趋于立体化。从以往传统的单机版杀毒，到网络版杀毒，再到全网安全概念的提出，反病毒技术已经由孤岛战略延伸出立体化架构。这种将传统意义的防病毒战线从单机延伸到网络接入的边缘设备；从软件扩展成硬件，是在长期的病毒和反病毒技术较量中的新探索。

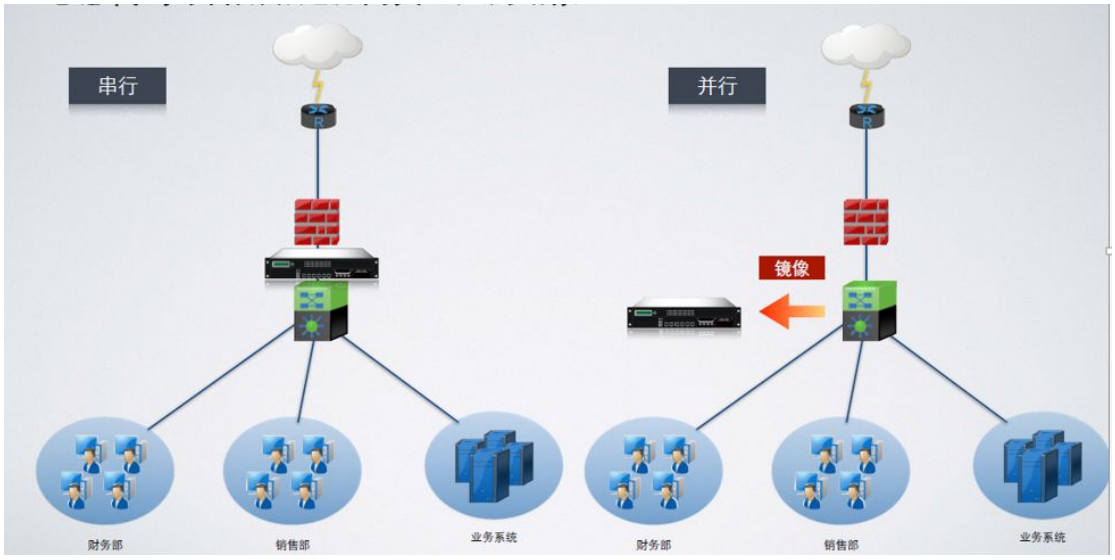
（2）流扫描技术广泛使用于边界防毒。为了能够更好地避免病毒（特别是蠕虫病毒）的侵袭，边界防毒方案将会得到更加广泛的采用。它在网络入口处对进出内部网络的数据和行为进行检查，以在第一时间发现病毒并将其清除，有效地防止病毒进入内部网络。由于边界防毒需要在网络入口进行，那么就会对病毒的查杀效率提出极高的要求，以防止明显的网络延迟。于是，流扫描技术应运而生。它是专门为网络边界防毒而设计的病毒扫描技术，面向网络流和数据包进行检测，大大减少了系统资源的消耗和网络延迟。

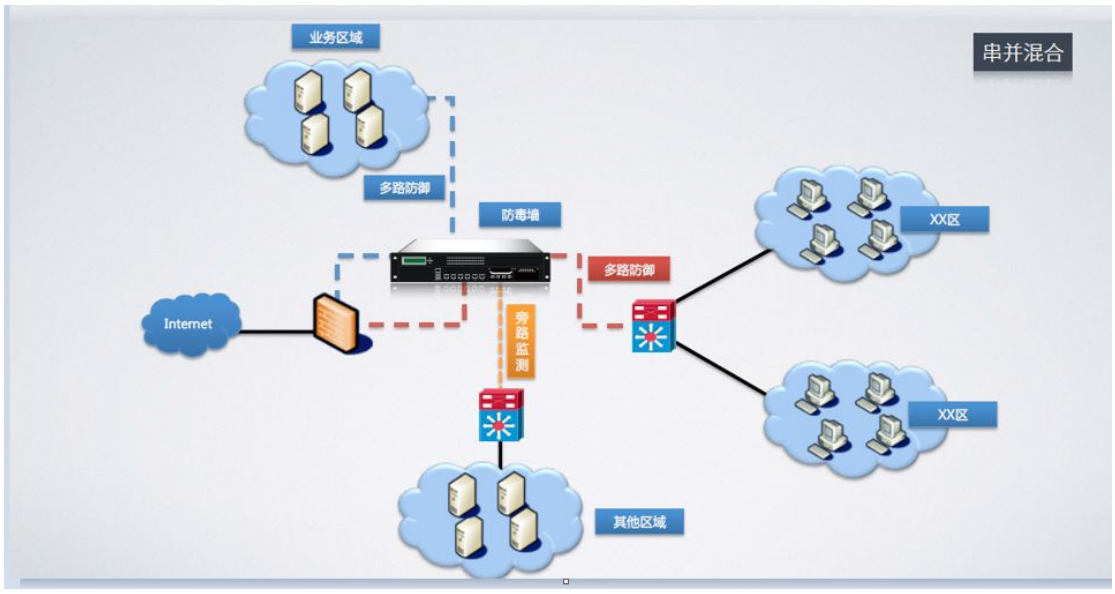
3.2 防毒墙部署

合理的划分安全域是网络安全可控性目标的重要基础，把安全机制落实到相关的保护范围和对象，根据安全责任范围和安全策略范围，对网络系统分不同安全域实施不同级别的安全保护。在合理划分安全域的基础上对域边界进行可控性管理建设，成为病毒防御体系建设的又一关键点。

现阶段面对新复合型病毒、蠕虫病毒、木马通讯、口令嗅探的攻击，传统的解决方案完全丧失了对内部网络的控制能力，最典型的就是面对蠕虫的攻击，只要蠕虫在内部网络被触发，网络管理人员往往只能在顾此失彼中感叹蠕虫的可怕，面对蠕虫病毒的大面积破坏行为，完全丧失了对网络的安全控制能力，这种现象的最根本原因就是缺乏域边界的控制措施。

为了改变这种被动现状，加强边界的控制和防御能力，我们在网络的边界部署网关级边界病毒过滤设备江民防毒墙（MDG），进行有效的蠕虫和新复合型病毒的主动防御。通过域边界江民防毒墙（MDG）的部署，当内部网络再触发某蠕虫病毒，进而对整个网络发起攻击的时候，MDG 可以将其控制在某个安全域之内，避免其进一步大面积扩散，造成整个网络瘫痪等事件的发生，为网络管理人员提供了有效的网络病毒控制手段和能力，为内部网络病毒防御的可控性目标提供了有力的技术保障。





边界病毒防护示意图

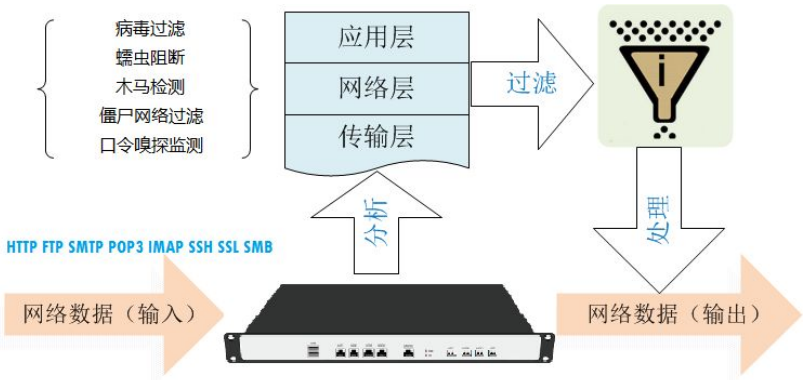
网络边界的病毒防御建设提高了网络管理人员对网络的安全控制能力，有效的防御了病毒、木马、蠕虫等病毒威胁在内部网络不同区域内的破坏、扩散，切断了其在网络内部的传播途径。

第 4 章 江民防毒墙概述

4.1 产品综述

江民防毒墙（MDG）是一款专注于防范网络恶意代码，网络恶意行为威胁的过滤网关产品。可有效拦截/监控诸如病毒传播、蠕虫攻击、木马通讯、僵尸网络、口令探测等当前活跃的多种网络威胁。区别于传统的防火墙/防毒墙，MDG 将自己的防范目标定位于恶意代

码和恶意网络通讯，专注于对恶意代码和恶意网络通讯的识别和拦截，是帮助企业防范恶意代码，完善网络安全防护的有利工具。



江民防毒墙（MDG）综合采用数据包结构分析、网络行为分析、特征识别、模式匹配、流量控制与自动抑制、协议分析、深度内容分析、专业防病毒识别、蠕虫过滤、木马通讯阻断、口令嗅探识别、全透明桥接等技术，实现对网络威胁数据的精确过滤。

江民防毒墙（MDG）定位于网络恶意江民防毒墙，提供全面的网络威胁防御。江民防毒墙（MDG）产品面向企业级用户，包括政府、金融、电信、教育、企业等网络用户。

4.2 产品特点

- **灵活接入，即插即用。**江民防毒墙（MDG）支持 INLINE/ONLINE 两种接入模式，即插即用，适应各种复杂的网络环境，支持 VLAN（包括非对称 VLAN）、HA、单臂路由等网络环境。支持无 IP 接入，产品本身不需要设置任何地址即可进行过滤监控。
- **IPV4/IPV6 双栈支持。**江民防毒墙（MDG）全面支持 IPv4 和 IPv6 网络环境。
- **性能优秀，多路监控。**江民防毒墙（MDG）采用多核并行处理、重构网卡驱动、TCP/IP 协议栈等技术，保证系统的高效过滤性能；支持多路监控，并且可同时支持 INLINE/ONLINE 模式的监控。
- **动态识别应用协议。**江民防毒墙（MDG）支持非端口定义的协议识别，通讯服务端无论采用什么端口，都能正确识别 HTTP/FTP/SMTP/POP3/IMAP/SSH/SSL/SMB 等多种应用层协议。
- **精确的病毒过滤能力。**江民防毒墙（MDG）针对网络传播病毒进行全面高效的专项过滤，精确识别邮件病毒、文件传输病毒、网页病毒等，防止病毒通过最常见的传播途径进入受保护网络。
- **强大的蠕虫过滤能力。**江民防毒墙（MDG）采用入侵防御（IPS）技术、IP/端口/数据

包封锁技术，优化了蠕虫识别机制，不仅可过滤已知蠕虫，还可以在未知蠕虫爆发时进行拦截。

- **强大的木马通讯监控。**江民防毒墙（MDG）内置数千种木马通讯协议识别特征，可监控多数常见的木马通讯，并且，识别库不断再升级，以识别新型木马，包括手机木马。
- **高效的反钓鱼机制。**江民防毒墙（MDG）内置数十万有效的钓鱼网址和恶意网址，同时内置数百种针对各种浏览器的溢出攻击特征，防范网络钓鱼攻击和浏览器溢出攻击。
- **防范口令探测能力。**江民防毒墙（MDG）可对常用的网络服务如：SMTP/POP3/IMAP/FTP/

  HTTP/SSH/TELNET/SMB 等进行口令探测的活动均可被监测，并可触发相应的阻断动作，防止口令探测活动的持续进行。并预留接口进行二次开发，对用户专有的网络服务实现口令探测监控。
- **保障自身安全工作。**江民防毒墙（MDG）通过多种措施保障自身安全工作：通过专有安全操作系统避免漏洞攻击；通过自动抑制网络流量，防止 DoS 攻击造成拒绝服务和性能下降；通过加密和认证的安全管理防止管理失控。

4.3 主要功能

（1）蠕虫过滤

蠕虫可以利用电子邮件、文件传输等方式进行扩散，更主要的特点是利用系统的漏洞发起动态攻击。近几年蠕虫造成的危害越来越大，可以导致系统严重损坏和网络瘫痪。如尼姆达（Nimda）、飞客（Conficker）、蠕虫王（Slammer）、冲击波（Blaster）、震荡波等。

根据蠕虫的特点，江民防毒墙（MDG）从 OSI 的多个层次进行处理。在网络层和传输层过滤蠕虫利用漏洞的动态攻击数据，在应用层过滤利用正常协议（SMTP、HTTP、POP3、FTP、IMAP、SMB 等）传输的静态蠕虫代码。

江民防毒墙（MDG）所独有的抗蠕虫攻击技术（Anti-Worm）处于国际领先地位，能够全方位抵御所有已知蠕虫病毒的攻击，弥补了国内同类产品空白。这一技术标志着，江民防毒墙（MDG）不仅可以过滤静态蠕虫代码，而且能够阻断蠕虫的动态攻击（包括所引发的病毒传播、后门漏洞、DoS/DDoS 攻击等）。这样，可以实现全面防御蠕虫的目的。

（2）病毒过滤

这里的病毒过滤是指静态型病毒（例如 CIH）、邮件病毒（例如求职信、美丽杀手、爱

虫、Mydoom）、特洛伊木马、网页恶意代码的过滤等。

对于网页浏览（HTTP 协议）、文件传输（FTP 协议）、邮件传输（SMTP、POP3 协议）等病毒，基于专门的病毒引擎进行查杀。对邮件病毒，可以定义对病毒的处理方式，决定清除病毒、删除附件、丢弃等操作，发现病毒时通知管理员、收件人、发件人等操作。

江民防毒墙（MDG）具有卓越的病毒查杀能力，能够对多种应用协议（SMTP、HTTP、POP3、FTP 等）所传递的数据进行病毒过滤。江民防毒墙（MDG）采用多引擎技术，能够100%地检测出目前“流行病毒名单”上的病毒。

（3）木马行为监测

一个完整的木马程序包含控制端和被控端。控制者通过操作被控端窃取大量机密或个人隐私信息。江民防毒墙（MDG）采用多重特征匹配、模式匹配和规则算法，对网络数据流实时解析，检测出的木马信息包括主机源 IP 地址、MAC 地址、源端口、目的 IP 地址、目的端口、木马类型、危害等级等信息。

（4）口令嗅探攻击监测

近几年帐号及口令外泄事件时有发生，越来越多的攻击手段也更加明确恶意攻击者的最终目的是要获得核心系统的最高权限，进而更加的肆意妄为。因此，对于企事业单位信息系统的账户及口令态势现状，俨然需要提升到一个新的高度，实现对各项信息系统帐户口令的恶意探测及暴力破解等非法行为的实时阻断与监控。江民防毒墙（MDG）通过对信息系统所依赖的网络服务进行协议识别，并深入分析协议层数据包内帐户信息传输状态，进而做到对帐户及口令的有效防御措施，最终实现对信息系统帐户安全的态势分析与全面掌控。

（5）僵尸网络检测

僵尸网络构成了一个攻击平台，控制者利用这个平台可以发起各种各样的恶意攻击，可以导致整个基础信息网络或者重要应用系统瘫痪，也可以导致大量机密或个人隐私泄漏，还可以用来从事网络欺诈等其他违法犯罪活动。江民防毒墙（MDG）采用特征匹配、模式匹配和规则算法，对网络数据流实时解析，检测出僵尸网络发动拒绝服务攻击、发送大量垃圾邮件、窃取计算机上的有用信息、滥用网络资源等恶意的黑客行为，详细信息包括主机源 IP 地址、MAC 地址、源端口、目的 IP 地址、目的端口、僵尸类型、危害等级、僵尸服务器域名等信息，通过检测信息可以找出内部网络中被种植了“僵尸程序”的“僵尸计算机”以及僵尸的行为。

（6）安全管理方式

对江民防毒墙（MDG）的管理支持 https 加密通讯的 Web 管理方式，界面直观、操作简

便、易于理解。此外还支持 console 方式的本地管理，以及 ssh 加密方式的远程维护管理。

为避免对江民防毒墙（MDG）设备的管理权限滥用，增加安全性，可设定允许访问江民防毒墙（MDG）设备的 IP 地址范围。管理员根据权限进行划分，管理用户按性质可划分为：系统维护员（超级用户）、配置管理员、策略审计员、日志审计员等。

（7）特征库自动升级

通过和多家 ISP 合作，建立了有效的恶意代码云监控网，江民防毒墙（MDG）通过不断更新过滤特征码来保持与攻击数据特征的同步。根据更新策略，用户可通过 HTTP 或 FTP 方式从公网服务器自动更新特征码。